a fingerprint scanner, a radio frequency identification (RFID) reader, a device-to-device reader, a smartphone, a wearable device, a biometric reader, a face recognition device, a voice recognition device, a heartrate monitor, or any combination thereof.

8. The security holster of claim **1**, wherein the device condition sensor includes a global positioning system (GPS), a force device condition sensor, an accelerometer, a sound detection device condition sensor, a frequency detection device condition sensor, a microphone, a camera, a speaker, or any combination thereof.

9. The security holster of claim **1**, wherein the computing device is configured to determine, based on authentication data from the requesting user, authentication data from the authorized user, the device condition data, or any combination thereof, if the security device is tampered with while the security device is in the locked configuration.

10. The security holster of claim **1**, wherein the computing device includes a processor configured to capture log data including one or more timestamped actions of locking, unlocking, accessing, tampering the security device, or any combination thereof.

11. The security holster of claim **1**, wherein at least one of the computing device, the device condition sensor, or the access authentication assembly is configured to communicate, via a network, to a pre-determined support group including a primary user, a designated user, a dispatch service, an emergency response unit, a third party system, an internet-of-things (IoT) device, or any combination thereof.

12. The security holster of claim **11**, wherein the at least one of the computing device, the device condition sensor, or the access authentication assembly is configured to communicate to the pre-determined support group via the network and a control device operably coupled to both the network and the pre-determined support group.

13. The security holster of claim **12**, wherein the control device is configured to perform one or more actions of:

receiving a notification that a request to access to the firearm or a distress signal predefined to be indicative of an emergency is detected;

sending an indication to the security holster whether the pre-determined support group determines that an emergency exists; or

sending a notification to the security holster that a support action is provided for the authorized user by the predefined support group.

14. The security holster of claim **1**, wherein the device condition sensor is operably coupled to a user monitoring device of the authorized user associated with the security holster.

15. The security holster of claim **14**, wherein the user monitoring device included a microphone, a radio, a body camera positioned on the authorized user, or any combination thereof.

16. A computer-implemented method for regulating access to a firearm secured within a security holster, the method comprising:

performing at least one of:

detecting a request to access the firearm secured within the security holster by a requesting user, and

detecting a distress signal predefined to be indicative of an emergency;

in response to the at least one of detecting the request to access the firearm or detecting the predefined distress signal, activating a user monitoring device of an authorized user associated with the security holster and notifying a predefined support group associated with the authorized user;

receiving an indication from the predefined support group, whether the emergency exists; and

in response to receiving the indication that the emergency exists, receiving a notification that a support action is provided for the authorized user by the predefined support group.

17. The method of claim **16**, wherein the pre-determined support group includes a primary user, a designated user, a dispatch service, an emergency response unit, a third party system, an internet-of-things (IoT) device, or any combination thereof.

18. The method of claim **16**, wherein the support action provided by the pre-determined support group includes:

providing information based on data received from the user monitoring device of the authorized user;

sending instruction to the authorized user;

providing information requested by the authorized user; or

any combination thereof.

19. The method of claim **16**, further including:

determining if the requesting user is the authorized user associated with the security holster based on authentication data from both the requesting user and the authorized user;

in response to determining the requesting user is the authorized user, allowing access to the firearm secured within the security holster; and

in response to determining the requesting user is not the authorized user, maintaining the security holster in a locked configuration to prevent access to the firearm.

20. The method of claim **16**, further comprising:

in response to determining the requesting user is not the authorized user, detecting at least one of tampering or movement of the security holster based on authentication data from the requesting user, authentication data from the authorized user, the device condition data, or any combination thereof.

* * * * *